

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS

1. (currently amended)

A computer-readable medium ~~memory~~ storing an electronic certificate data structure, the data structure comprising:

content data specifying an attribute delegation from an identified issuer to a certificate subject, and

an electronic signature of said issuer for confirming the content data;

wherein the content data includes ~~including~~ a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid.

2.(currently amended)

A computer-readable medium ~~memory~~ according to claim 1, wherein said certificate subject is generically any subject whereby said attribute is delegated to any subject capable of showing said condition to be satisfied, the particular subject of said condition being explicitly identified in the content data.

3. (currently amended)

A computer-readable medium ~~memory~~ according to claim 1, wherein said certificate subject is specifically identified in the content data.

4. (currently amended)

A computer-readable medium ~~memory~~ according to claim 3, wherein said particular subject is not separately specified but is implicitly said specifically-identified certificate subject.

5. (currently amended)

A computer-readable medium~~-memory~~ according to claim 3, wherein said particular subject is explicitly identified.

6. (currently amended)

A computer-readable medium~~-memory~~ according to claim 1, including multiple said conditions in predetermined logical relationship.

7. (currently amended)

A computer-readable medium~~-memory~~ according to claim 6, wherein said logical relationship is explicitly stated.

8. (currently amended)

A computer-readable medium~~-memory~~ according to claim 6, wherein said logical relationship is not explicit but is implicitly an AND relationship.

9. (currently amended)

A computer-readable medium~~-memory~~ according to claim 1, wherein said content data further includes certificate validity data concerning at least one of:

a date range identifying the period over which the certificate is valid;

the location of a certificate revocation list that should be checked before the certificate is used;

the location where a one-time use permission can be obtained or the certificate re-validated;

said content data being structured into fields with the validity data and said condition or conditions being held in the same field.

10. (currently amended)

A computer-readable medium~~-memory~~ according to claim 1, wherein the certificate has substantially the same form as an SPKI certificate data structure with said condition or conditions being held in a ~~the~~ validity field of the certificate data structure.

11. (currently amended)

Apparatus for generating an electronic certificate data structure, the apparatus comprising:

a data handling arrangement for assembling content data specifying an attribute delegation from an identified issuer to a certificate subject, and including a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid; and

a signature arrangement for generating an electronic signature of said issuer over said content data.

12-13. (cancelled)

14. (previously presented)

Apparatus according to claim 11, wherein the data handling arrangement is arranged to cause said certificate subject to be specifically identified in the content data.

15. (previously presented)

Apparatus according to claim 14, wherein the data handling arrangement is arranged to cause said particular subject to be implicitly specified in said content data as said specifically-identified certificate subject.

16. (previously presented)

Apparatus according to claim 14, wherein the data handling arrangement is arranged to cause said particular subject to be explicitly identified in the content data.

17. (previously presented)

Apparatus according to claim 11, wherein the data handling arrangement is adapted to permit multiple said conditions to be included in the content data in predetermined logical relationship.

18. (currently amended)

Apparatus according to claim 11, wherein the data handling arrangement is arranged to organise said content data into substantially the same form as an SPKI certificate data structure with said condition being held in a validity field of the certificate data structure.

19. (currently amended)

A reduction engine for verifying the existence of a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said reduction engine comprising:

a trust-chain verifier for combining justified attribute delegations to form said trust chain, at least one said attribute delegation being justified on the basis of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and

a trust-chain branch control arranged to require the trust-chain verifier to establish a branch of said trust chain upon the trust-chain verifier using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer.

20. (currently amended)

A reduction engine according to claim 19, adapted to handle a said conditional certificate data structure in which said certificate subject is specifically identified in the content data.

21. (currently amended)

A reduction engine according to claim 20, adapted to handle a said conditional certificate data structure in which said particular subject is not separately specified but is implicitly said specifically-identified certificate subject.

22. (currently amended)

A reduction engine according to claim 20, adapted to handle a said conditional certificate data structure in which said particular subject is explicitly identified.

23. (currently amended)

A reduction engine according to claim 19, adapted to handle a said conditional certificate data structure including multiple said conditions in predetermined logical relationship.

24. (currently amended)

A reduction engine according to claim 19, adapted to handle a said conditional certificate data structure that has substantially the same form as an SPKI certificate with said condition being held in a validity field of the certificate.

25. (currently amended)

A trust chain discovery engine for finding a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said discovery engine comprising:

a trust-chain builder for seeking to build up said trust chain using justified attribute delegations at least one of which is justified on the basis of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and

a trust-chain branch control arranged to require the trust-chain builder to seek to build a branch of said trust chain upon the trust-chain builder using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject

must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer.

26. (currently amended)

A trust chain discovery engine according to claim 25, adapted to handle a said conditional certificate data structure in which said certificate subject is specifically identified in the content data.

27. (currently amended)

A trust chain discovery engine according to claim 26, adapted to handle a said conditional certificate data structure in which said particular subject is not separately specified but is implicitly said specifically-identified certificate subject.

28. (currently amended)

A trust chain discovery engine according to claim 26, adapted to handle a said conditional certificate data structure in which said particular subject is explicitly identified.

29. (currently amended)

A trust chain discovery engine according to claim 25, adapted to handle a said conditional certificate data structure including multiple said conditions in predetermined logical relationship.

30. (currently amended)

A trust chain discovery engine according to claim 25, adapted to handle a said conditional certificate data structure that has substantially the same form as an SPKI certificate with said condition being held in a validity field of the certificate.